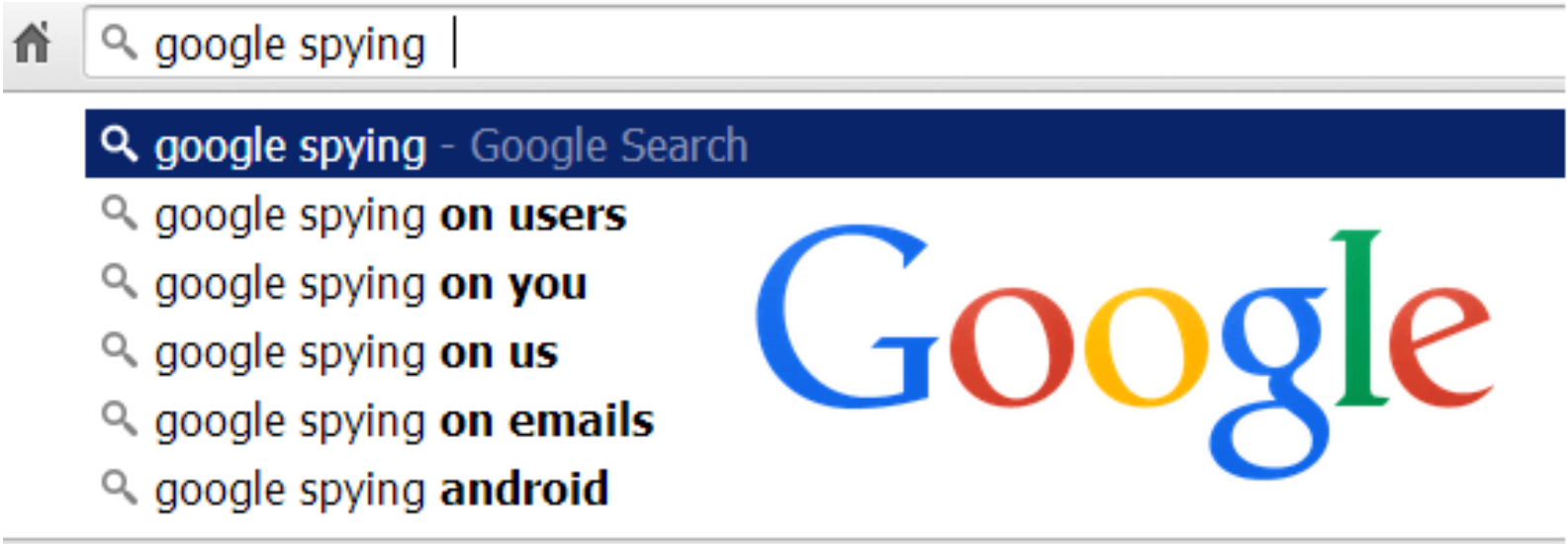
OK GOOGLE, DEGOOGLIZZAZIONE!

Perché è necessario e urgente liberarsi di Google (e come cominciare a farlo).



Wu Ming

INDICE

1. A day in your life (Google lo sa)

Ti svegli dopo un sonno di sei ore. Hai dormito male, sonno leggero e agitato. Google lo sa: lo ha rilevato dall'accelerometro e dal microfono nel tuo smartphone.

Dall'analisi della rete a cui sei connessa sa pure che non eri a casa tua, ma in un appartamento dall'altra parte della città e, dal registro dei tuoi spostamenti, sa pure che da circa un mese ti ci rechi almeno un paio di volte a settimana.

Google sa chi vive in quella casa, perché il GPS del suo smartphone indica giornalmente la sua presenza lì. Conosce bene quella persona, come conosce te. Sa che non fa parte della tua cerchia di amici ristretti, perché il suo numero non è nelle loro rubriche e molto raramente si trova negli stessi posti che loro frequentano. Sa che vi siete registrati a vicenda in rubrica qualche mese fa, ma solo negli ultimi tre avete iniziato a chiamarvi spesso.

Ieri sera avete visto un film sulla Chromecast. Ovviamente Google sa qual era il film e poiché i dati GPS indicavano che eravate entrambi in casa e non vi siete mossi, deduce che probabilmente eravate in salotto.

Sa pure che all'altra persona il film non doveva interessare molto, perché mentre lo stavate guardando non faceva che giocare con un videogame sul suo smartphone Android.

Grazie al DNS Google sa che, appena alzata, come ogni mattina, hai controllato le news sul solito sito. Android e Chrome glielo confermano.

Dall'archivio delle tue abitudini di lettura degli ultimi anni, Google sa che le notizie relative alle occupazioni abitative sono di tuo interesse, ma che leggi in dettaglio solo quelle che parlano di sgomberi. Dall'analisi dei testi delle tue email sa che ne parli anche con amici e conoscenti e che manifesti crescente preoccupazione per le dichiarazioni di un certo assessore. Dall'analisi dei movimenti del tuo dito sullo schermo sa quali titoli di notizie hanno attirato la tua attenzione anche se poi non li hai letti, e ritiene che se in questi titoli fossero state presenti determinate parole la probabilità che tu li aprissi sarebbe stata maggiore.

Alle otto hai percorso un certo tragitto in città. Google lo sa, sempre grazie al GPS e per via del distacco dal wi-fi dell'appartamento.

Dall'analisi di percorso e velocità Google deduce che lo spostamento sia avvenuto in bicicletta. Sa che poi sei entrata in un certo bar, probabilmente a fare colazione, dato che ti sei trattenuta mezz'ora, e che lì ti sei connessa al Wifi

sbagliando il captcha tre volte, deducendone che forse sei ancora un po' addormentata, poiché di solito li becchi al primo colpo.

Google rileva che poi ti sei agganciata alla rete della biblioteca e hai cercato un certo oggetto che ritiene ti debba interessare molto, poiché la ricerca ti ha portato a girar diversi siti, finendo per trovarlo su quello di un certo negozio online dove l'hai acquistato fornendo la tua solita carta di credito. Ritiene statisticamente probabile che possa trattarsi di un regalo per una delle tue migliori amiche, quella che compirà gli anni tra un paio di settimane e che a sua volta acquista spesso oggetti dallo stile simile.

Poi scrivi un testo su un'app che hai scaricato dal Play Store e anche se non è un'app di Google, l'azienda ha accesso alla tastiera di Android e quindi è comunque in grado di comprendere cosa hai digitato, incluse le parti cancellate. Il testo contiene passaggi in inglese e dalla velocità con cui le hai digitate capisce che è una lingua che pensi di padroneggiare bene, anche se in realtà nota che ripeti sempre gli stessi errori di grammatica.

A quel punto ricevi una chiamata da una persona che nella tua rubrica è registrata come «Mamma», e parlate per cinque minuti. Google rileva una certa ansia nella tua voce e ciò gli conferma quel che aveva già presunto: c'è tensione tra te e tua madre.

Lo aveva dedotto da diversi fattori, tra cui il gran numero di volte che non rispondi alle sue chiamate anche se sei a casa, e dal fatto che durante le feste sei lontana da lei e non la chiami.

Più tardi ti scatti un selfie con alcuni amici e dai metadati della foto Google può sapere dove e quando è stata scattata. Analizzando l'immagine può identificare le persone ritratte così come il tipo d'abbigliamento, dal quale può dedurre gusti e marche, dato utile per confermare cose che già sa sul tuo e loro livello economico.

Arriva la sera e fai una corsa nel parco ascoltando musica e indossando un braccialetto elettronico che registra le tue attività come il tipo di andatura, il battito cardiaco ecc. Non ci hai mai fatto caso, ma sia l'app per la musica in streaming sia quella del braccialetto avvisavano da qualche parte che i dati sarebbero stati condivisi con «terze parti», ossia partner commerciali. Ciò che non potevi sapere è che tra questi vi è pure Google, che quindi conosce anche i tuoi dati fisiologici, le tue abitudini sportive, oltre ovviamente ai tuoi gusti musicali.

Google sa anche che sei una persona romantica e riflessiva, perché traspare da ciò che cerchi online nei momenti liberi; sa che fai letture impegnate, e che hai un debole per i panda.

Non possiamo affermare con certezza quali rilevazioni Google faccia costantemente, quali *una tantum* a scopo "sperimentale" e quali invece siano rilevazioni che tecnicamente potrebbe fare ma in realtà non esegue. Non possiamo dirlo, perché quel che accade nei server di Google lo può sapere solo Google, e perché i suoi strumenti sono spesso chiusi e non permettono una verifica trasparente.

Quali che siano le rilevazioni effettivamente fatte, sappiamo che Google ci osserva attraverso innumerevoli canali, e registra le nostre attività. La mole dati a cui Google ha accesso gli permette di ricostruire la vita delle persone in modi che nemmeno un social network potente e pervasivo come Facebook può sognare.

2. Siamo un terreno di conquista commerciale

Quando si parla di *Big Tech*, ossia delle principali multinazionali tecnologiche, la prima constatazione è che mai, nella storia, poche aziende commerciali private di dimensioni tanto colossali erano riuscite a diventare parte inestricabile della vita di miliardi di persone, e in modo così diffuso e capillare.

Lo scenario, già problematico, di poche grandi aziende che detengono il potere su tecnologie ritenute ormai indispensabili risulta ancor più inquietante *invertendo i fattori* della constatazione: mai prima d'ora ogni minimo dettaglio della vita di miliardi di persone era stato portato a un tale livello di mercificazione, fino ad annoverarlo fra i terreni di conquista di poche colossali aziende private.

Parliamo dunque di *big data*, ossia dell'estrazione di informazioni dettagliate dalle nostre attività, dalle nostre *vite*, a fini – non solo – commerciali.

Quello dei *big data* è un circuito che si autoalimenta per allargare costantemente i propri margini. C'è uno scambio impari tra noi persone/utenti e le aziende che grazie ai dati che forniamo sviluppano tecniche e strumenti atti a legarci maggiormente ad esse, per estrarci ancor più informazioni.

Ciò avviene attraverso soluzioni tecniche e psicologiche note e meno note, scelte di design applicate a software che sfruttano la *gamification* per indurci a interagire maggiormente o attraverso l'imposizione di standard *de facto* cui risulta assai difficile sfuggire. La ricerca di gratificazione data dai like o l'impossibilità di rinunciare a Whatsapp, per esempio.

Qui possiamo osservare il circuito che si autoalimenta: abbracciare acriticamente servizi e strumenti imposti dall'industria tecnologica si rivela sempre più una scelta obbligata, poiché più questi vengono adottati, meno spazio vien dato alle alternative libere: i documenti di testo sono quasi sempre realizzati in Word; per condividere i file di lavoro nella maggioranza dei casi la scelta cade quasi sempre su Google Drive, Dropbox e poco altro; per conoscere le attività di un'associazione è necessario stare su Facebook; se si vuol creare un account email la scelta dei provider è indirizzata verso un ristretto numero di colossi (Google su tutti), e così via.

Con l'«*Internet of things*» (d'ora in poi IoT), ossia col sempre maggior numero di oggetti costantemente connessi, non si farà che estendere i campi d'estrazione: automobili elettriche che comunicano costantemente una miriade di dati, lampadine di cui l'azienda saprà se sono accese o spente, asciugacapelli, televisori, frigoriferi, biciclette, attrezzi da cucina, orologi da polso ecc. È facile prospettare lo sviluppo di innumerevoli tecnologie IoT da parte di aziende anche medio-piccole che verranno poi assorbite dai grandi colossi, e non è fantascienza immaginare un futuro prossimo in cui sarà difficile, se non impossibile, procurarsi oggetti che non trasmettano informazioni alle Big Tech.

Questo è il primo problema: più strumenti e piattaforme commerciali utilizziamo, più ci precludiamo un'indipendenza da essi.

Tra le maggiori aziende che ruotano attorno a questa massiccia estrazione di dati, quella più imponente è sicuramente Google. Non è certo l'unica azienda-vampiro, e molte delle osservazioni presenti in quest'articolo potrebbero essere applicate anche ad altre, le più note delle quali sono parte dell'acronimo GAFAM: Google, Apple, Facebook, Amazon e Microsoft. Tuttavia, se ognuna di queste aziende si è evoluta a partire da settori specifici non necessariamente incentrati sull'estrazione dati, Google nasce fin dal principio come *puro recettore di informazioni*, ed è quella che nel tempo ha ampliato le proprie capacità estrattive nei modi più diffusi e capillari.

3. "Sappiamo" ma non sappiamo

Che «Google ci guarda» è un sentire comune, ma a ben vedere si tratta di una mera *conoscenza latente*: sappiamo che certi banner pubblicitari appaiono solo dopo che abbiamo fatto determinate ricerche, e ci viene costantemente ricordato che i cookie per accedere a diversi siti sono usati per profilarci, ma al di

fuori di questi pochi esempi e del concetto generale, ci sfuggono la varietà e il funzionamento dei meccanismi con cui avviene l'estrazione di dati.

Questo è il secondo problema: in una società sempre più dipendente da tecnologie informatiche, la scarsa conoscenza del funzionamento di tali strumenti ci pone più o meno nella posizione di analfabeti che devono muoversi in un mondo sempre più basato sulla lingua scritta.

A differenza dell'alfabetizzazione, però, l'informatizzazione può avvenire a livelli molto più diversificati, e lo dimostra il fatto che sia possibile esser al tempo stesso utenti smaliziati che si muovono agilmente tra mail, fogli elettronici, sistemi di chat, impostazioni dello smartphone e applicazioni di ogni tipo, ma non esser in grado di scrivere una sola riga di codice e non aver la minima idea di come facciano questi strumenti a funzionare.

Il fatto è che essere utenti che sanno utilizzare gli strumenti non basta, perché la mancanza di *comprensione* del loro *funzionamento profondo* ci relega nella condizione passiva di semplici utilizzatori finali, privi delle conoscenze necessarie a sviluppare un approccio critico per non farci sopraffare.

Periodicamente appaiono notizie su fughe di dati personali, applicazioni malevole, problemi legati alla privacy e preoccupanti episodi di censura e abuso di potere da parte delle Big Tech. Eppure, nonostante tutti questi segnali concordino nel prospettare scenari preoccupanti, l'adozione di strumenti alternativi non è ancora diventata un fenomeno diffuso. Questo a causa delle due problematiche qui esposte: da un lato la posizione di dominio dei prodotti delle Big Tech e dall'altro il fatto che l'insufficiente conoscenza di tali strumenti impedisce di comprendere *davvero* i pericoli che quel dominio comporta.

Tuttavia, il dominio delle Big Tech non è affatto ineluttabile, ma non sarà possibile limitare le derive oppressive delle tecnologie informatiche senza uno sforzo di apprendimento il più collettivo possibile su come queste funzionano.

Non si può certo pretendere che si diventi tutti programmatori, e nemmeno che si abbandonino in modo drastico e immediato strumenti e piattaforme conosciute a favore di strumenti liberi con cui non si ha (ancora) dimestichezza, ma è comunque necessario correre al più presto ai ripari e avviare *subito* un processo di apprendimento ed adozione di tecnologie libere.

4. Come è potuto succedere

È utile riassumere brevemente come si sia arrivati alla situazione attuale. Negli anni Novanta l'arrivo di Internet e del web fu accolto da un vento di cyber-

utopismo trasversale e generalizzato, spesso tanto entusiasta da convincersi che l'estendersi della rete avrebbe portato *automaticamente* a un'informatizzazione spontanea delle masse, e conseguentemente a forme di democratizzazione planetaria per via tecnologica. Tale entusiasmo nasceva dall'incontro tra le visioni utopistiche e anarchiche diffuse tra informatici, hacker e attivisti e l'ingenua curiosità della maggioranza delle persone verso tecnologie dal sapore vagamente fantascientifico.

Negli stessi anni la contrapposizione tra Microsoft e i sistemi operativi liberi GNU/Linux già conteneva tutti i conflitti futuri tra grandi aziende e software libero: grazie ad accordi commerciali stretti da Microsoft coi maggiori produttori di computer mondiali, quando si acquistava un nuovo PC, come sistema operativo vi si trovava preinstallato Windows (e come ben sappiamo, questa situazione si è protratta fino ad oggi). Fu così che la potenza di fuoco dell'azienda di Redmond minò in modo drammatico l'adozione di sistemi operativi GNU/Linux per uso personale. Oggi Windows è di fatto lo standard principale per i computer domestici.

A cavallo del 2000, l'entusiasmo per le nuove tecnologie portò alla nascita di esperienze come quella di Indymedia, ma pure all'esplosione della bolla speculativa delle dot-com, che fece fallire innumerevoli imprese digitali. Se gli anni Novanta erano stati caratterizzati da un alto tasso di sperimentazione che riguardava sistemi operativi, piattaforme online di comunicazione, formati digitali e siti di diverso tipo capaci di nascere e morire in tempi rapidissimi, gli anni Zero portarono a maturazione l'esperienza precedente con la nascita di un gran numero di strumenti e piattaforme commerciali la cui fortuna continua ancor oggi.

Giusto per far qualche esempio noto, oltre a riconfermare le realtà già esistenti più solide**, come Amazon (1994) e Google (1998), gli anni Zero videro la nascita di iTunes (2001), Wikipedia (2001), Skype (2003), Facebook (2004), Gmail (2004), Yelp (2004), YouTube (2005), Google Maps (2005), Twitter (2006), Google Docs (2006), Spotify (2006), lo Smartphone (2007 – primo iPhone), DropBox (2007), Chrome (2008), AirBnB (2008), Zalando (2008) WhatsApp (2009), Uber (2009), Pinterest (2009), Instagram (2010), Tablet (2010 – primo iPad).

Grazie alla sempre maggiore diffusione di Internet e al continuo aumento di servizi online, in quegli anni l'accesso al web iniziò a diventare esperienza quotidiana anche al di fuori dell'ambito lavorativo per molte persone che non provenivano dal mondo dell'informatica o dell'hacking.

Se gli ambienti hacktivisti prospettavano un futuro di utenti con un approccio all'informatica critico e attivo, le nuove piattaforme commerciali compresero che il vero affare era l'estrazione di informazioni dagli utenti, e che ciò poteva essere ottenuto fornendo strumenti gratuiti e subito funzionanti, che richiedessero pochissimo impegno per capire come usarli. La maggior parte degli utenti, dunque, si approcciò al web in quegli anni trovando la disponibilità di applicazioni e piattaforme gratuite realizzate con grandi capitali, ampiamente pubblicizzate, esteticamente piacevoli e molto facili da usare. Se negli anni '90 era considerato normale dover pagare per servizi come l'email, ora un'intera generazione di utenti veniva educata ad abbracciare strumenti e servizi gratuiti, e a ritenere inevitabile il dover dare in cambio l'accesso ai propri dati.

Il software libero realizzato da una galassia eterogenea di realtà prive di grandi capitali, che richiedeva uno sforzo di comprensione maggiore e in alcuni casi era a pagamento, risultava decisamente meno attraente.

Il risultato è che col tempo, a parte poche meritevoli eccezioni ascrivibili al mondo dell'hacking vero e proprio, anche gli ambienti inizialmente più critici e attenti hanno finito con l'adottare gli stessi strumenti commerciali che avrebbero dovuto avversare. Ci siamo dunque trovati con realtà anticapitaliste che comunicano le proprie iniziative su Facebook, si scambiano le email con Gmail, comunicano con Whatsapp e si scambiano documenti con Google Drive.

In modo altrettanto preoccupante, diversi enti pubblici hanno affidato le proprie comunicazioni (anche interne!) agli strumenti delle Big Tech. Oltre a consolidare queste preoccupanti situazioni di monopolio privato ed a contribuire alla diffusione del *data mining* nelle nostre vite, l'adozione acritica di questi mezzi ha contribuito a consolidare la falsa idea che questo modello – grande azienda di capitali che fornisce strumenti centralizzati su scala globale – sia l'unico possibile.

5. Software libero

Uno degli aspetti frustranti di quest'abbandonarsi in massa alle tecnologie traccianti è che le alternative non mancano affatto. Non solo non si è mai smesso di realizzare software libero ma anzi, quest'ultimo copre una grande percentuale del software prodotto su scala mondiale.

Non è certo possibile condensare in poche righe la natura, filosofia e storia del software libero, del movimento internazionale che lo supporta e men che meno esporne le diverse sfaccettature, ma giusto per illustrarne i tratti essenziali basterà dire che si tratta di programmi il cui codice-sorgente è aperto e distribuito

liberamente. Questo permette a chiunque ne abbia la capacità di verificarne il funzionamento, collaborare a migliorarlo, modificarlo e crearne versioni alternative.

Si tratta di una differenza notevole rispetto al software commerciale, che invece è chiuso, intoccabile e protetto da copyright. Volendo fare un paragone automobilistico, il software libero è come un'automobile di cui si può aprire il cofano, vedere il motore, ripararlo, modificarlo o addirittura assemblarne uno nuovo, mentre il software chiuso è come un'automobile il cui cofano è sigillato e si può solo tentar di dedurre come funzioni esattamente, senza averne mai la certezza.

Se il software commerciale è sempre controllato dall'azienda che lo produce, il software libero è realizzato e mantenuto da un ventaglio di realtà che spaziano dal singolo programmatore che lavora in autonomia all'azienda etica che mette a disposizione gratuita il software che ha creato guadagnando invece dalla vendita di servizi o tramite donazioni, fino a intere community dedite allo sviluppo collettivo di un intero sistema operativo.

La filosofia stessa con cui viene realizzato il software libero stimola costanti revisioni da parte di intere comunità globali e fa sì che questo sia spesso molto più efficiente di quello commerciale, tanto che anche molti strumenti commerciali che utilizziamo quotidianamente contengono, sotto i propri cofani, ampie porzioni di software libero.

Se da un lato le aziende commerciali hanno imposto il proprio dominio tramite una potenza di fuoco difficile da contrastare, dall'altro lato è pur vero che si sono imposte anche grazie ad un certo tipo d'attenzione all'utente medio, in termini di semplicità e immediatezza di utilizzo, che il mondo del software libero non sempre è stato in grado di fornire.

Si tratta tuttavia, anche in questo caso, di una classica situazione ricorsiva: la minor adozione di strumenti liberi da parte della maggioranza degli utenti è al tempo stesso causa e conseguenza del loro insufficiente adattamento alle esigenze del grande pubblico.

Un esempio su tutti può essere il caso di **Jabber/XMPP**, tecnologia di chat che esiste dal 1999. Non ha nulla da invidiare ai vari Whatsapp, iChat e simili, ma non è mai stata in grado di imporsi. Molto probabilmente una maggior adozione iniziale avrebbe contribuito non poco a consolidarne la diffusione e spronare un maggior numero di persone ad attivarsi per levigarne alcune caratteristiche che ancor oggi ne rallentano la diffusione.

Va però tenuto conto che alla base di certe caratteristiche che possono rendere meno immediato l'utilizzo del software libero vi sono spesso ragioni tecnico-etiche che *devono* essere mantenute tali. Prendiamo ancora l'esempio di Jabber/XMPP: per usare Whatsapp, Viber o Telegram bastano pochi click sullo smartphone e questi, dopo aver preso possesso del nostro numero di telefono e di quello di tutti i nostri contatti, funzionano immediatamente. Al contrario Jabber/XMPP richiede la creazione di un account e poi i contatti vanno inseriti manualmente. Se nel primo caso regaliamo i dati di tutti i nostri conoscenti e tutti i nostri dialoghi in cambio di uno strumento subito funzionante, nell'altro abbiamo uno strumento che richiede sì alcuni settaggi iniziali, ma in cambio non invade la privacy di nessuno.

Ad ogni modo, il mondo del software libero non è mai stato a guardare ed ha costantemente maturato e migliorato la propria attenzione verso l'utenza media. **Mastodon** è uno degli esempi di software libero che, mirando ad equilibrare le proprie caratteristiche complesse e un utilizzo il più possibile semplificato, riesce ad attrarre numeri importanti.

6. I mille tentacoli di Google

Di solito chi utilizza un certo strumento vuole solamente che sia facile e pratico nel fare ciò che deve. Questo atteggiamento può certo bastare nel caso di strumenti che per loro natura sono finiti in sé stessi, come un martello, una bici o una macchina da scrivere, ma non è più sufficiente quando si ha a che fare con strumenti informatici, perché questi ultimi, sotto la loro parte visibile, possono comportarsi in modi che non approviamo e che contribuiscono a ingabbiarci sempre più.

Nel caso di Google, ad esempio, le informazioni che inseriamo attivamente nei suoi strumenti sono la parte *visibile* di ciò che stiamo consegnando: i testi che digitiamo: una parola cercata sul motore di ricerca, il contenuto di un'email, gli appuntamenti inseriti sul calendario, una città cercata su Google Earth, ma anche i pdf caricati su Google Drive, le foto ed i tracciati GPS… Sono dati che grossomodo chiunque si rende conto di consegnare all'azienda.

Ma è la parte *invisibile* quella più consistente, composta da miriadi di informazioni personali che Google carpisce anche quando non ci rendiamo nemmeno conto che stiamo inviando dati, anzi, anche quando non ci rendiamo nemmeno conto che stiamo usando Google.

Per esempio: quando si naviga su un *qualunque* sito internet è molto probabile che questo contenga componenti che trasmettono informazioni a Google. Un'estensione per il browser **Firefox** chiamato **Cloud Firewall** permette di bloccare questi elementi. È particolarmente istruttivo navigare sui siti che si frequentano regolarmente ma con Cloud Firewall impostato per bloccare *tutti* gli elementi traccianti o anche solo quelli di Google: da alcuni siti scompaiono i banner pubblicitari, in altri non appaiono più i commenti, oppure possono scomparire i video e le immagini, o non ci sono più i soliti font né gli sfondi; diversi pulsanti scompaiono o smettono di funzionare; certe pagine non sono nemmeno più navigabili, perché basate completamente sui servizi delle Big Tech. Basta un pomeriggio di navigazione con Cloud Firewall attivato per rendersi immediatamente conto di *quanta* parte di Internet sia materialmente in mano a queste poche aziende.

Ma non finisce qui: Google mette a disposizione di programmatori, web designer e professionisti vari una lunga serie di servizi tecnici – un elenco è disponibile su Wikipedia – a cui solitamente non si presta molta attenzione e con cui abbiamo a che fare quotidianamente, come i captcha (verifica in due passaggi per entrare in un sito web), il login con l'account di Google, oppure Google Analytics. Sono tutti strumenti (tentacoli) con cui Google estende le proprie capacità di estrazione dati. Chi usa Android molto probabilmente sincronizza i propri contatti tramite Google e quindi gli consegna tutta la propria rubrica. Ci sono app di notizie che si appoggiano su Google News e dunque gli forniscono informazioni sugli argomenti che ci interessano ecc. Alcuni di questi strumenti, addirittura, possono essere essenziali al funzionamento stesso di Internet, come il Google Public DNS sul quale vale la pena spendere qualche parola.

7. Il Google public DNS

Ogni sito internet è identificato da un proprio codice univoco chiamato *indirizzo IP* che funziona più o meno come un numero di telefono: inserisci il codice IP nel browser e questo si connette alla pagina desiderata. Per esempio, questo post si trova su *Giap*, il cui indirizzo IP è 136.243.238.37. Se si inserisce tale indirizzo nella barra del proprio browser, premendo invio si aprirà proprio *Giap*.

Gli indirizzi IP però sono scomodi da ricordare: «Ho letto un gran bell'articolo su 136.243.238.37» non suona granché bene… Per questo fin dai primordi del web è stata sviluppata una rete di server chiamati DNS, Domain Name System,

ognuno dei quali contiene una sorta di rubrica indirizzi pubblica che collega gli indirizzi IP a nomi più semplici da memorizzare, i nomi di dominio, ossia gli URL a cui siamo abituati che iniziano con www e finiscono con punto qualcosa. È grazie al DNS che possiamo usare www.wumingfoundation.com al posto di una scomoda sequenza di numeri.

Qui arriva la parte che ci interessa: quando digitiamo un URL o clicchiamo un link il nostro device non fa altro che interrogare uno o più server DNS chiedendo loro l'indirizzo IP corrispondente e permettendo la connessione. È evidente che chi gestisce un server DNS saprà sempre che un dato computer o smartphone ha cercato un certo sito, e ciò indifferentemente dal computer o modello di telefono usato, dal sistema operativo, browser e motore di ricerca. Ebbene, il servizio DNS più grande e usato al mondo e che facilmente troviamo impostato di default nei nostri device appartiene proprio a Google.

Google dichiara di cancellare parte dei dati di navigazione di cui viene a conoscenza entro 48 ore, ma che un'altra parte la conserva a tempo indefinito. In sostanza siamo di fronte a un'azienda che oltre a possedere un quasi-monopolio sulle ricerche online detiene pure il controllo di grandissima parte dei dati sulla navigazione anche di chi non usa il suo motore di ricerca.

Ebbene, ci vuol poco a cambiare il server DNS che il nostro device interroga di default.

8. Fonti differenti ma analisi unica

Ricerche online, traffico DNS, movimenti del mouse, posizioni GPS, reti a cui ci si connette, rubriche telefoniche, tasti digitati sulla tastiera: sono informazioni di natura diversissima, e prese singolarmente possono avere un'importanza relativa, ma tutti insieme e in mano ad un'unica azienda possono essere incrociati fra loro ed è a questo punto che divengono estremamente importanti (per l'azienda) e pericolosi (per noi).

Per esempio, durante una banale navigazione in Internet le diverse fonti a cui Google attinge permettono di ricostruire ogni minimo dettaglio della nostra navigazione: possiamo fare una ricerca su Google (1) che ci rimanda a un sito che contiene componenti di Google (2), banner pubblicitari di Google (3) e un video di YouTube (4). Per accedere al sito potremmo doverci loggare con l'account di Google (5) e passare per il suo captcha (6). All'interno poi troveremo un link ad un secondo sito e cliccandoci useremo il DNS di Google (7). Tutto questo potrebbe esser stato fatto con Chrome (8) da un cellulare Android (9) della linea Pixel (10),

prodotta dallo stesso Google. Più sono gli strumenti di Google che utilizziamo e più dettagliata sarà la sua conoscenza delle nostre attività.

È inevitabile che alcune attività online vengano tracciate dai fornitori di servizi; ecco perché oltre alla comprensione degli strumenti e all'utilizzo delle alternative libere, anche recidere i diversi tentacoli è di importanza fondamentale, poiché l'accumulazione centralizzata di una grande mole di dati non permette solamente di ricostruire reti di contatti, abitudini e spostamenti ma, come si è già accennato, può spingersi ancor più a fondo permettendo una schedatura sociale, economica, psicologica e politica di ogni soggetto.

Qui si apre un campo di discussione vastissimo in cui l'analisi dei dati va a toccare aspetti tecnici, semantici, psicologici, comportamentali, sociali e in cui strumenti e formule vengono continuamente sperimentati, scartati, modificati ed affinati. Le modalità e i criteri con cui questi dati vengono analizzati non sono di pubblico dominio e al massimo possiamo presumerli o dedurli.

Chi presta attenzione alle notizie tecnologiche sa bene che negli anni Google ha continuamente sviluppato – e acquistato aziende che producono –strumenti di vario genere utili ad acquisire più informazioni o analizzarle con maggior dettaglio, e che tra il personale di Google vi sono psicologi, sociologi, esperti di statistica e di altri campi grazie ai quali vengono sviluppati algoritmi di analisi sempre più raffinati, capaci di dedurre statisticamente tendenze sopite e debolezze psicologiche di ogni singolo utente arrivando a stilarne un ritratto completo e dedurne la *forma mentis*. E non solo la nostra: anche quelle di chi fa parte della nostra rete sociale.

Ciò significa che liberarsi dagli strumenti di Google non è sufficiente se viene fatto da un singolo utente, senza coinvolgere anche gli altri componenti delle nostre cerchie sociali: Google saprebbe comunque chi ti ha inserito in rubrica e chi ti chiama dal proprio telefono Android, saprebbe il tuo compleanno perché altri lo hanno inserito nei loro calendari e saprebbe quando la tua solita compagnia si trova tutta assieme nel vostro locale preferito grazie ai loro GPS ecc.

Google potrebbe anche condurre esperimenti mirati, come far funzionare appositamente male l'assistente vocale in determinati momenti solo per misurare l'ansia e nervosismo che questo genera in noi, analizzando la nostra voce, oppure esponendo gli abitanti di regioni diverse a versioni differenti di una stessa notizia per studiarne le reazioni. Le tecnologie dell'informazione in mano a società di capitali, dunque, non si limitano a trasformare il mondo in una rete di

sorveglianza a cielo aperto, ma trasformano ogni persona in una cavia per esperimenti psicologici e sociali e rendono amici, parenti e vicini *delatori involontari*, fonti di informazioni su di noi.

9. Il problema non sono necessariamente i dati, ma chi li detiene e ciò che vuol farne

Google guadagna dalla vendita dei nostri dati. O meglio: vende aggregazioni e analisi dei nostri dati. Quali siano i dati che vende dipende da scelte commerciali e, almeno in teoria, da limiti legali. In teoria, non può vendere dati sensibili capaci di ricondurre gli acquirenti alla singola persona, ma quali siano esattamente questi limiti è argomento tecnico-giuridico assai complesso: ad esempio, vendere anonimi tracciati GPS di percorsi fatti al mattino in bicicletta da attiviste napoletane di sinistra tra i 25 e 30 anni con un debole per i panda, potrebbe essere perfettamente legale.

Che siano venduti o no, tuttavia, questi dati sono comunque informazioni presenti nei database di un'azienda privata che in futuro potrebbe analizzarli con nuovi strumenti, venderli legalmente, farseli rubare o essere obbligata a comunicarli a governi e agenzie di intelligence. Già ci sono segnali in questo senso: il governo degli Stati Uniti ha tentato di imporre ad Apple di fornirgli gli strumenti per poter accedere a qualunque iPhone, generando l'assurda situazione in cui una multinazionale si è atteggiata a paladina "buona" della privacy.

La cessione di questi dati e analisi ad aziende private o enti di sorveglianza può portare a scenari che non è esagerato definire distopici. Solitamente, chi difende questo stato delle cose o minimizza il problema se ne esce con la massima fascistoide secondo cui «*chi non ha nulla da nascondere non dovrebbe preoccuparsi»,* non facendo altro che deviare il discorso dal punto della questione: il problema non è necessariamente il contenuto dei dati di per sé, ma chi li detiene e ciò che vuol farne!

La consegna di tutti i nostri dati permette di redigere profilazioni che per quanto raffinate esse siano, non escludono mai i bias di chi li realizza. In sostanza, chi ritiene di «non aver nulla da nascondere» non fa che affidare il giudizio sulla propria intimità a multinazionali e poteri governativi, che ovviamente la giudicheranno coi propri parametri culturali e in base ai loro interessi.

Tu che leggi sei una persona "irreprensibile"? Poco importa: gli scenari che potresti incontrare in un futuro caratterizzato da un uso ancor più massiccio dei big data sono comunque tremendi. Le scuole migliori (privatizzate) potrebbero

rifiutare l'iscrizione dei tuoi figli perché in base alle analisi preventive effettuate tramite big data non rientrano nei loro standard; enti di polizia potrebbero metterti in una lista di "attenzionati" perché classificano come pericoloso chiunque legga un determinato sito nonostante contenga contenuti legittimi; la tua compagnia di assicurazioni potrebbero aumentarti la polizza in base ai dati fisiologici ottenuti dai tuoi attrezzi sportivi; aziende potrebbero negarti l'assunzione perché nella tua rete di contatti vi sono sindacalisti a loro non graditi, e così via.

Sono scenari potenziali, si, ma che si trovano dietro l'angolo: a dividerci da loro ci sono forse alcune reticenze e barriere legali, ma è in questa direzione che il capitalismo spinge con forza, ed è un futuro che può tentare di realizzarsi in diversi modi: abituando le persone a consegnare volontariamente i propri dati, oppure per vie legali o in altre forme ancora, pertanto ogni segnale che punti in quella direzione va tenuto sott'occhio. In quest'emergenza coronavirus, ne abbiamo notati parecchi.

10. Decentrare, federare, adottare standard aperti

Liberarsi dalle maglie di Google e limitarne lo strapotere è un processo che può essere attuato solo adottando software libero, ma sostituire strumenti su cui non abbiamo il controllo con strumenti trasparenti non basta ad evitare la formazione di nuovi enti accentratori. Questo perché numerosi strumenti si appoggiano a servizi forniti da terzi: allo stato attuale, è irrealistico prospettare uno scenario in cui ogni singola persona/utente gestisce da sé un proprio server casalingo su cui girino chat, email o quant'altro.

Parimenti, lo scenario – non meno irrealistico – in cui diversi servizi globali siano sostituiti da una moltitudine di alternative indipendenti farebbe venir meno diversi dei vantaggi che offrono alcune piattaforme globali.

La soluzione prospettata da diverse piattaforme libere per fornire al tempo stesso i vantaggi delle reti autonome e la comodità delle grandi piattaforme consiste nell'applicazione di due concetti: *decentralizzazione* e *federazione*, con cui si intende la creazione di reti interconnesse tra loro («federate») di diversi fornitori di servizio indipendenti («decentralizzati») attraverso una tecnologia di comunicazione comune.

Un esempio di strumento federato e decentralizzato già noto e usato da anni è l'email: gli indirizzi di qualsiasi provider difatti possono dialogare con tutti gli altri indirizzi mail esistenti.

Il concetto di fondo consiste nel dare la priorità non a singoli strumenti alternativi ma a protocolli aperti che possano a loro volta essere utilizzati tramite strumenti liberi, ossia consolidare standard diffusi e utilizzabili da chiunque senza obbligare nessuno a legarsi ad un certo fornitore di servizi specifico

Per fare un paragone: Whatsapp è uno strumento chiuso che può essere usato esclusivamente passando da Whatsapp stesso (se ti togli da Whatsapp perdi tutte le chat Whatsapp); al contrario Mastodon è uno strumento aperto privo di un "centro di comando", che permette a chiunque di crearsi il proprio server con le regole che preferisce.

Lo stesso concetto può essere applicato in diverse forme: scegliere ad esempio di sostituire Google Drive passando in massa a Dropbox aiuterebbe ben poco. Al contrario si può scegliere uno dei numerosi provider che usano il software libero **Nextcloud**: anche qui, lo stesso software, ma messo a disposizione da realtà diverse e indipendenti fra loro.

La preferenza per gli standard aperti può essere declinata anche sui singoli file: ognuno, ad esempio, può scegliere l'editor di testi che preferisce ma se ci si impone di usare solo editor che possano lavorare in formato **.odt** (Opendocument, l'alternativa libera dei file .doc) ecco che ciò porterebbe pure diverse aziende commerciali ad adottare standard aperti.

È dunque possibile passare da una situazione che vede un servizio di Google impostosi come riferimento unico globale, tipo Google Maps, ad una situazione con applicazioni diversissime e indipendenti che hanno come riferimento comune le ricche mappe di **OpenStreetMap**.

Si tenga anche conto che in alcuni casi ciò può richiedere un acquisto o una donazione, perché realizzare e mantenere certi servizi può avere un certo costo.

11. Propaganda invisibile e mirata

Il banner "targetizzato" che appare dopo che abbiamo fatto una certa ricerca, per quanto fastidiosissimo, è solo la forma più grossolana e visibile di utilizzo dei nostri dati a scopo propagandistico-commerciale.

Le cose diventano molto più ambigue quando la propaganda si manifesta in modi meno espliciti. Già adesso, per intenderci, Google cambia da utente a utente l'ordine dei risultati che mostra sul suo motore di ricerca, ma è nei possibili sviluppi futuri delle tecnologie che coinvolgono le intelligenze artificiali (IA) che il quadro si fa più inquietante. I testi scritti automaticamente dalle IA. si stanno facendo sempre più indistinguibili da quelli realizzati da esseri umani ed è dunque

possibile prospettare che dei crawler – programmi automatizzati che scrutano i contenuti presenti in rete – collegati ai database di Google e a IA specializzate in scrittura, potranno di fatto essere utilizzati come giornalisti-robot capaci di generare in tempi rapidissimi articoli di news altamente targetizzati, coi quali sarebbe possibile propagandare una stessa informazione in modi differenziati, per far passare un medesimo concetto a persone di orientamenti totalmente opposti, differenziando gli articoli in forme adatte ad essere maggiormente accettate da ciascun singolo utente.

Se il concetto da far passare fosse che «il soggetto politico X è inaffidabile», a una stessa ricerca le persone già ostili a tale soggetto potrebbero vedere notizie che rafforzano la loro avversione, mentre alle persone simpatizzanti le stesse notizie potrebbero essere mostrate in forme più ambigue e sfumate, in modo da scavalcare le difese e generare comunque sospetti e dubbi.

La colonizzazione dei quotidiani da parte delle aziende di *data mining* potrebbe avvenire in forme non dissimili da quelle già applicate dalla *gig economy* in altri settori: così come AirBnB non "possiede" gli appartamenti che affitta, Google potrebbe non possedere mai i quotidiani, ma legandoli irrimediabilmente a sé attraverso i propri servizi e detenendo il potere sulle piattaforme utilizzati, controllarli di fatto. Attualmente Google avvantaggia i siti di news che adottano un suo formato di pubblicazione chiamato AMP, legando così a sé queste testate, spingendoci a preferirle rispetto ad altre. Se cerchi una notizia su Google vengono mostrate prima le testate che usano AMP, mentre articoli forse più completi e documentati vengono relegati alla pagina 3, che raramente viene aperta.

Nel caso di Cambridge Analytica, che ha riguardato la Brexit e le presidenziali statunitensi del 2016, è stato osservato che il massiccio uso di news dal taglio personalizzato e distribuite nei feed personali di Facebook può aver influenzato l'opinione pubblica in maniera rilevante ma non controllabile, mostrando contenuti di propaganda mirata di cui non è stato possibile tenere traccia, dato che scomparivano poco dopo esser stati letti (Facebook non registra la cronologia di quali annunci vengono mostrati ad un utente). In quel caso si è trattato perlopiù di post a pagamento che gli utenti più sgamati avrebbero potuto identificare per ciò che erano, ma cosa succederà quando non sarà più possibile comprendere se una data notizia è targetizzata su di me o no?

Oggi la cosa viene ancora svolta con un alto tasso di intervento umano, tramite persone che si occupano materialmente di scrivere materiale di propaganda in seguito trasmesso da bot o pubblicato come annuncio a

pagamento ma non è così distante il futuro in cui potremmo interagire con bot indistinguibili da utenti reali, con tanto di voce e immagine video generata artificialmente, che dialogheranno con noi esponendoci le loro "opinioni" utilizzando sottigliezze discorsive e psicologiche tagliate apposta per far breccia nella nostra psiche, grazie al fatto che, a nostra insaputa, ci conoscono perfettamente.

Propaganda commerciale e propaganda politica si rivelano di fatto indistinguibili e ciò non è un mero accidente causato dalla tecnologia: si tratta della naturale evoluzione delle logiche capitalistiche, che vedono nell'estrazione di valore dalle attività umane la premessa per manifestarsi appieno nella loro evoluzione successiva, ossia il capitalismo della sorveglianza.

12. Capitalismo della sorveglianza

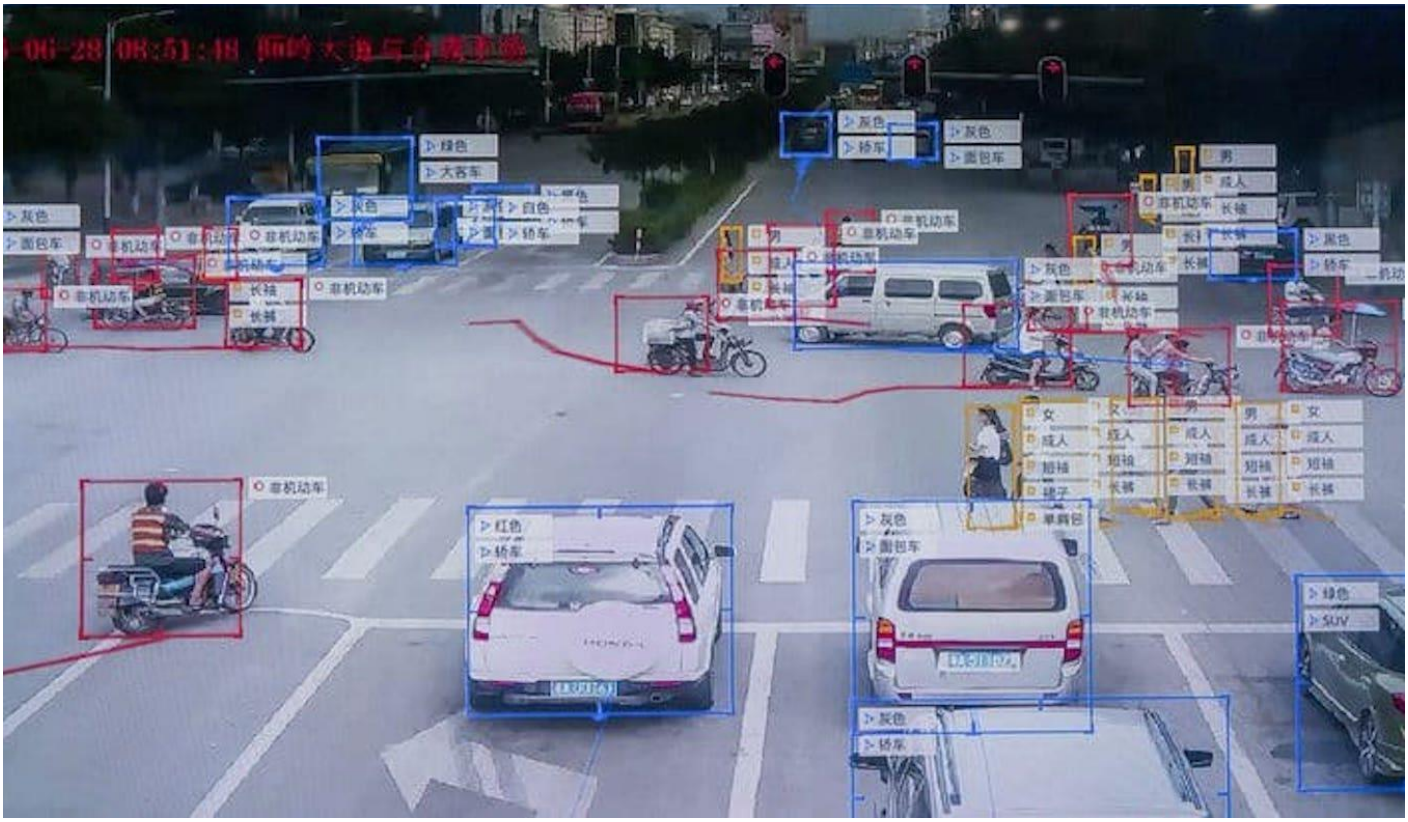
Il capitalismo della sorveglianza è già realtà. Semplicemente, le forme in cui si realizza non si sono ancora espresse al massimo. E se le sue manifestazioni materiali più evidenti sono quelle legate all'IoT, è soprattutto agli aspetti sociali derivanti dalla loro implementazione che bisogna prestare attenzione, e soprattutto alla *domanda di sicurezza* che oggi viene costantemente alimentata (c'è sempre un'emergenza utile alla bisogna).

Basta solo ipotizzare che le reti di telecamere già esistenti nelle nostre città vengano implementate – come sta avvenendo in altre parti del mondo – con tecnologie di riconoscimento facciale a loro volta connesse con profilazioni ottenute da fonti come Google, per rendersi conto del potenziale livello di controllo a cui andiamo incontro.

Tutto ciò può già essere osservato in Cina, dove le tecnologie per la sorveglianza sono utilizzate in maniera massiccia: a Shanghai, megaschermi collegati a sistemi di riconoscimento facciale posti nei pressi di passaggi pedonali, mostrano il documento d'identità di chi attraversa con il rosso. Una forma moderna di gogna pubblica.

Le stesse tecnologie vengono impiegate in banche, aeroporti, alberghi e bagni pubblici. Se ne vedono le applicazioni più estreme nello Xinjiang, dove tra sistemi di riconoscimento facciale, scansioni biometriche e sistemi di sorveglianza a terra ed aerea (coi droni) la regione abitata dalla minoranza uigura è diventata un vero e proprio carcere a cielo aperto in cui i movimenti di ogni persona sono monitorati, registrati e analizzati.

La *domanda di sicurezza* di cui sopra, che da tempo plasma la vita nelle nostre città, tra richieste di installazione di videocamere ovunque, militari impegnati nell'operazione «Strade sicure», controlli di vicinato, droni che sorvolano le manifestazioni, sistemi di riconoscimento veicolare e accessi monitorati mostra tendenze che potrebbero evolversi in scenari non dissimili da quello appena descritto per lo Xinjiang. L'esempio più recente cui abbiamo assistito è stato quello dei lockdown imposti per il Covid-19, di dubbia utilità per lo scopo esplicito (contenere la diffusione del virus) ma utili a quello implicito, ossia far avanzare di qualche passo l'accettazione di controlli autoritari e sospensione delle libertà.



Non si tratta di scenari unilateralmente calati dall'alto: sono accolti e addirittura auspicati da una fetta della popolazione intrisa di ideologia securitaria o, più spesso, auspicati parzialmente, senza rendersi conto dello scenario nel suo complesso.

Ciò avviene nella presunzione che un monitoraggio costante di ogni attività umana e sociale serva a renderci non solo più sicuri ma pure più efficienti, in una continua ricerca di «ottimizzazione» tramite sorveglianza e punizione.

Basta pensare al livello di controllo che diverse aziende applicano sui propri dipendenti, sempre più spesso obbligati a registrare ogni loro minima attività, a strisciare il badge all'entrata e all'uscita del gabinetto perché qualcuno possa stilare statistiche sui tempi della nostra pisciata media ecc.

Ecco, in soldoni, la peggior deriva a cui stiamo andando incontro: un futuro che è già qui, in cui raccolta di dati, profilazione, monitoraggio e sorveglianza senza limite sono legati a doppio filo con l'ideologia legalitario-securitaria diffusa nella società social-mediatizzata.

13. Degooglizziamo le nostre vite

È in riferimento a tutto questo che risulta interessante, utile e preziosa la campagna di *degooglizzazione*, che invita a non consegnare più a Google nessun momento delle nostre vite. Si tratta di una campagna informale portata avanti in modo spontaneo, singolarmente o in gruppo, da un gran numero di hacktivist in tutto il mondo.

Rispetto ad altri processi simili e altrettanto importanti ma più semplici da avviare – come l'adozione di piattaforme alternative a Facebook, Instagram, Twitter e Whatsapp – la rimozione di Google, per via della vastità e varietà di campi informatici che tocca, è una pratica da svolgersi in più fasi, toccando ogni volta con mano e imparando tutti gli aspetti tecnici che è necessario conoscere.

La degooglizzazione, in sostanza, aiuta ad allenarsi per portare avanti l'impegno, sempre più necessario, a sviluppare una maggior consapevolezza informatica.

Una fonte consigliabile è **Framasoft**, associazione francese nata per diffondere l'adozione di software libero. Da alcuni anni Framasoft porta avanti un progetto di degooglizzazione offrendo molti strumenti alternativi e suggerimenti utili.

Conclusione

Siamo già in ritardo e bisogna recuperare il tempo perduto. Si tratta di un percorso a volte scomodo – «la degooglizzazione non è un pranzo di gala», ha scritto Wu Ming su Bida tempo fa – ma la cui necessità è sempre più impellente.

L'impegno dev'essere il più attivo, diffuso e collettivo possibile: esistono decine di hacklab e migliaia di persone capaci di aiutare in questo percorso, che ha perlomeno il vantaggio di poter essere effettuato a scaglioni:

■ sostituire il motore di ricerca di Google con **DuckDuckGo** e **SearX** è operazione che si fa in un attimo;

■ sostituire Google Maps con **OsmAnd** o **Pocket Earth** pure;

■ stessa cosa per passare da Chrome a **Firefox**;

■ per aprire una nuova casella email con **Autistici** o **Tutanota** è gradita una donazione, nel primo caso, o richiesto un piccolo pagamento, nel secondo;

per cose più complesse, come passare da Windows a una distribuzione GNU/Linux o altro, ci vuole un po di più tempo, via via fino a cose più complesse come sostituire il sistema operativo del cellulare.

Seguire le news tecnologiche e i forum di informatica dovrebbe diventare un'attività costante. Inevitabilmente ci saranno scazzi, si sbatterà il muso sul bisogno di cambiare abitudini, imparare l'uso di strumenti nuovi, aver a che fare con le diverse opinioni degli "smanettoni" su quale sia lo strumento alternativo migliore, ma il punto è tirarsi su le maniche e cominciare a lavorarci.

Subito.

Articolo pubblicato il 20/03/2020 su wumingfoundation.com

edicolaanonima.noblogs.org


Google
Spying on
you since
1998